ORF ISSUE BRIEF
NOVEMBER 2015
ISSUE NO. 113

Cyber Arms Race in Space: Exploring India's Next Steps

RAJESWARI PILLAI RAJAGOPALAN AND DANIEL A. PORRAS

ABSTRACT India's reliance on outer space has become critical in its social and economic growth stories in addition to its transformative impact in the national security context. With growing reliance comes vulnerability to adversarial attempts to harm India's capabilities, particularly from the new threat of cyber warfare. Even as countries including India have debated the need to develop certain counter-space capabilities, such as demonstration of an ASAT capability, no further tests have been carried out yet. With growing linkages between cyber and outer space domains, India should have a considered set of options that would protect its vulnerabilities in space. India has to be mindful of counter-space capabilities in its neighbourhood, such as anti-satellite missiles, lasers and jamming, and develop options to negate the impact of satellite communication interference.

INTRODUCTION

Following the 2007 anti-satellite (ASAT) test carried out by China, a number of countries including India began contemplating the necessity of demonstrating their own counter-space capabilities, particularly of the kinetic nature employed by China. Some states earnestly began to develop expensive missile technology that would be able to destroy a satellite in orbit. The need for such technology development stemmed from the traditional framework of deterrence: one actor will not commit a particular type of attack for fear of retaliation. Under this model, a successful ASAT demonstration is necessary to prevent an ASAT attack. However, to the great relief of many in the space community who worry about the proliferation of space debris, no further tests have been carried out thus far.[1] Unfortunately, this may not be a good sign.

Part of the reason for departing from kinetic ASATs is a growing trend in counter-space technology that is moving away from costly capabilities (such as a missile or a projectile that will physically destroy a satellite) and shifting towards cheaper (and possibly more dangerous) cyber attacks. Even a brief glance at recent news headlines will show that cyber attacks, popularly

known as "hacks", are becoming increasingly common. Large companies, international banks, power stations, and government agencies have been struck by a wide variety of virtual perpetrators. The actors behind these attacks have gone from being individuals with a computer and a criminal intent, to whole divisions of defence departments with specific national-security mandates. In this context, space systems have been identified as uniquely attractive targets because they are major conduits of information and strategic coordination. Over the last five years alone, the world has seen a significant spike in the intentional interference of satellites and their ground stations, including cases of jamming signals, eavesdropping and even taking full control of satellites for periods of time.[2] To make matters worse, the lines that define traditional actors have become blurred, with private hackers being recruited by governments to carry out cyber attacks, much like the buccaneers of yore.[3]

It is against this backdrop that Indian policy-makers and leaders must consider how to approach warfare in the digital age. Both outer space and cyber space are new dimensions that modern militaries rely on greatly but it is as yet unclear what vulnerabilities exist that might be exploited. No physical harm has yet been inflicted on a space system through cyber means but hackers have certainly begun probing the possibilities, sometimes with technology that is cheap and readily available. Terrorists and criminal organisations can, and indeed have already used these means. How much more sophisticated must the capabilities of global military superpowers be in comparison? For a country like India, which has highly developed space systems and whose infrastructure relies significantly on space capabilities, the question of developing protection against hacks is already answered: it is an absolute priority, particularly for its space networks. The next question is whether they should also be developing offensive cyber capabilities for striking the space systems of others. And if so, would it be prudent to demonstrate these capabilities?

SPACE SYSTEM VULNERABILITIES

At its core, a hack is simply the exploitation of a vulnerability in any given system. With space capabilities, there are three groups of weak points that can be exploited: the satellite itself, a ground station, or the end-user. Numerous studies have catalogued some of the means already in use to hack space systems and they have revealed some alarming vulnerabilities.[4]

The most common space cyber attack, though one might not think of it at first as a cyber attack *per se*, is jamming. This occurs when the signal from a satellite is overpowered by a stronger signal.[5] Between 2010 and 2012, for example, North Korea was accused of jamming South Korea's GPS signals for days at a time, affecting many planes, ships and personal devices.[6] While no lives were lost, these incidents created a great deal of economic and safety problems and exposed the vulnerabilities of human dependence on such systems. It also gave rise to significant concerns because the technology suspected of being used in these instances is widely available for less than US $50.

GPS signals can also be "spoofed," causing a satellite to track a false signal, thereby producing faulty data. With so many critical systems reliant on accurate data, it is not inconceivable that a cyber attack could be carried out that would interfere with GPS and impact major infrastructure sites such as banks, power grids and transportation. It is particularly alarming to think that an atomic power station might also belong to this list.

Jamming has also been used to prevent the transmission of foreign television signals into certain countries. There has recently been a huge jump in cases of satellite interference in the Middle East, causing considerable discussion among Member States of the International Telecommunications Union (ITU).[7] In particular, Iran has been accused of jamming certain news broadcasts, such as that of BBC's Persian TV, in order to prevent Western media from reaching domestic viewers.[8] This jamming was especially evident during the 2009 presidential elections

and the Arab Spring revolts.[9] Similarly, Qatar-based news broadcaster Al Jazeera's satellite signals were jammed by Egyptian authorities, forcing the news channel to change frequencies in order to provide continued service.[10] Such jamming results in widespread interference, disrupting the signal not only to domestic end-users but also to neighbouring countries. Iran has categorically denied these accusations, despite evidence that the signals causing the disruption originated within Iranian borders. It is worth noting that even if Iran were causing this disruption, it may not be a violation of international law because Iran could invoke its right to protect national security.

While jamming does emerge for all intents and purposes, as a form of hacking when most people think of hacking, they imagine using a computer to invade and command another system. These types of attacks have been around for years, displaying a significant amount of audacity even in the early stages of space cyber warfare. In 2011, a report by the US-China Economic and Security Review Commission reported that two US satellites had been compromised in 2007 and 2008 through a ground station in Norway. The attack, carried out via the internet, was traced to China.[11] Though the US government did not accuse anyone outright, it did say that the nature of the attack was linked with Chinese hackers and that it was consistent with policy documents published by China's military. The severity of the attack was especially alarming because, at least in the 2008 attack, the hackers were able to achieve "all steps required to command the satellite," though no harm was done.[12] Potentially, the hackers could have stolen data, redirected the solar panel array to destroy them or even moved the satellite to cause a collision. A third incident was reported in 2014 when a satellite operated by the US National Oceanic and Atmospheric Administration confirmed that a hacking on one of its satellites had been detected, though none of its data was compromised.[13] Again, though no official accusations were made, suspicions once again seemed to point to China. And though no harm was done, these incidents marked the emergence of systematic probing into the vulnerabilities of US satellite systems. Whether directly responsible or not, China has policy-makers concerned that counter-space offensive cyber operations are now an integral part of its overall defence policy.[14]

Predictably, the US has also signalled its willingness to use offensive cyber warfare where necessary. The leaking of President Barack Obama's Presidential Policy Directive 20, which asks intelligence officials to draw up a list of viable foreign targets for cyber attacks, would indicate that space systems will likely be targeted as the US ramps up its offensive cyber capabilities. While no specific examples of hacking have yet been assigned to the US government in terms of warfare, there is the example of the ECHELON programme, a sophisticated international eavesdropping system that can intercept telecommunications from all over the world, including those travelling via satellite, which demonstrates the extensiveness of US cyber capabilities being used to ensure its national interests.[15] The documents released by Edward Snowden in 2010 revealed numerous listening stations in countries such as Brazil, Germany, India and Japan.

Given Russia's extensive use of cyber warfare, it can probably be expected that they too are looking to leverage this technology in outer space.[16] Notably, reports have emerged that an independent group of Russian-speaking hackers, believed by some to be linked to the Russian government, has been using commercial satellites to exploit diplomatic and military agencies across the United States, China and Europe for eight years.[17] It should be noted that this group also targeted agencies in Russia, making the link to the government more tenuous. However, what seems to be clear is that the malware used to carry out attacks originated with a Russian government affiliate. It is, therefore, extremely likely that the Russian military will be capable of using similar software to advance their geopolitical interests.

All of these activities do not amount to the start of a cyber war but they certainly indicate

that cyber arms are being developed for offensive purposes and that countries need to inject more resiliency into their space systems. Opponents are carefully watching each other's moves to see what they may or may not be able to achieve by striking at space systems without actually causing any harm or incurring any consequences. While China, Iran, North Korea, Russia and the US have all had accusations laid against them regarding cyber attacks on space systems, there has not been a significant strike or attack that has led to an escalation of cyber warfare. Part of this may be because no one wishes to reveal their hand just yet, leaving all parties unsure about what the others can do. This situation could be seen as a virtual Mexican stand-off where the gunfighters are duelling in the dark during a thunderstorm.

Further complicating the situation is the entrance of non-state actors. Much of the expertise behind current cyber activities belongs to private actors, some of which could be termed criminals or terrorists.[18] These actors are capable of carrying out highly sophisticated and potent attacks, as clearly exhibited by the hacking group, Anonymous. For governments, this means that there is a ready pool of cyber mercenaries ready to engage in potential space cyber warfare. However, it is an uncomfortable reality that these parties may or may not be totally under the control of their government recruiters and, like the pirates of long ago, could become rogue actors with significant capabilities for cyber disruption.

And while there are numerous uncertainties about where cyber warfare will take geopolitics, what is clear is that the next phase of military readiness will likely involve preliminary hacking in order to weaken an opponent's defences and retaliatory capabilities. This, at the very least.

INDIA'S CYBER AND SPACE POLICIES

India has yet to actively commit itself to this new dimension of warfare. There is also far less clarity in terms of institutional and legal architecture to tackle the emerging threats in this domain. India's approach in this regard has been primarily national security-driven though it has undergone a shift lately with a focus on social harmony and cohesion as driving factors. Accordingly, new rules were brought in that required websites and service providers to remove objectionable contents if the government considered them "blasphemous" or "hateful" within 36 hours of notification.[19] While social harmony and cohesion are important drivers, they cannot negate the importance of freedom of speech, especially in a democracy like India. India has to be able to draw a fine balance between internet freedom and cyber warfare – a point that must be factored in as India redraws its policy on cyber issues. India also needs to bring back the focus on the protection of critical infrastructure as an important driving factor in its policy. Moreover, the national security-related threats in the form of cyber attacks are becoming more rampant and India must attend to this, both in its institutional and legal frameworks.

Recognising the increasing need to monitor and protect information systems, India came out with a national cyber security policy in July 2013. The policy, however, is just an initial step and a lot needs to be done in terms of both the legal and institutional architecture. The policy framework developed by the Department of Electronics and Information Technology (DeitY), Ministry of Communication and Information Technology, underlines the importance of information system in the overall growth story of India and hence the need to augment the defences against potential attacks. With a mission "to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation", the document lists several objectives including setting up of an "assurance framework for design of security policies," facilitating adoption and compliance of global best practices, strengthening of the regulatory framework that would ensure a secure cyberspace ecosystem, establishing a national and sectoral 24x7 threat monitoring as well as response and crisis management mechanism, creating a 500,000-strong workforce

over the next five years and providing fiscal incentives to businesses for implementing security policies and processes.[20] Also to be established is a 24X7 nodal National Critical Information Infrastructure Protection Center (NCIIPC) capable of predicting, preventing, protecting and responding to cyber incidents.[21] In March 2015, the Modi Government also designated the first cyber security chief within the Prime Minister's Office.[22] This is a much-required step but it cannot take away the importance of an overarching law or the institutional architecture that needs to be put in place. Two years since the policy was enunciated, little appears to have been done. Therefore, the 2013 policy looks good on paper, but it suffers from several lacunae. For one, it envisions every conceivable objective that it becomes difficult for the government to prioritise and take action. It is not clear whether it is a direct impact of the policy, but all companies are now required to have a Chief Information Security Officer and this is now a reality. However, even as India has a declared cyber security policy, it is still a rudimentary one and it is difficult to assume that the government has considered in any serious measure what cyber threats mean in the realm of outer space security.

On outer space, India is yet to formulate an open policy. Moreover, there is a growing disjuncture between India's rhetoric in international fora and the development of India's military capabilities in space. Official statements in the Parliament and international fora such as the Conference on Disarmament and other UN bodies reiterate India's traditional stand against weaponisation of space. On the other hand, India has already begun to put in place elements of an increasingly military space programme, probably driven by events such as the 2007 Chinese ASAT test. The launching of GSAT-7, India's first dedicated military satellite, for the Indian Navy in August 2013 is an indicator of things to come. The policy debate in instituting a tri-service aerospace command is also in recognition of the new realities in the neighbourhood. Thus, India's political masters and the military bureaucracy are finally beginning to assign an increasingly militaristic role to India's space programme but there is clearly no clarity or consistency on policy.

OPTIONS TO SECURE SATELLITES

With growing inter-linkages between cyber and outer space domain, India should consider a series of policy options that could compensate for India's vulnerabilities in the space domain. India needs to consider the growing counter-space capabilities particularly in its neighbourhood such as anti-satellite missiles, lasers and jamming.[23] India is yet to demonstrate any counter-space capability of its own although defence research and development agencies have reiterated their capability to do so should there be a political decision. India has to pay particular attention to the satellite communication, which may face several vulnerabilities. Any disruption or manoeuvring of satellite communications could potentially affect aerospace, military, civil aviation, oil and gas industries, among others. Hijacking a satellite control, disrupting or feeding wrong data are well-known means of disruption and this could affect India in economic and societal terms. Disruptions in communication satellites can also impact the operational integrity of military units in the field as well as cargo vessels out in high seas or airline safety and security.[24] These attacks could occur at the ground level on control stations or satellite launch facilities, or attacks could include those on sensors, antenna or on satellite communication links.[25] Challenges in India's neighbourhood are well-known. While much of China's capabilities, for instance, are being developed keeping the US as the prime target, implications for India cannot be overlooked.

India must have a considered set of practical options to negate the impact of satellite communication interference. One possible option is to harden the satellites, using designs, protection technologies and components that could make the systems more robust, thus making the satellites less vulnerable. Hardening is a route that has been particularly popular among militaries given what is at stake. Commercial

enterprises have been rather slow at embracing this option due to the cost factor.[26] A second option is redundancy by using backups. Attacking the backup module would require a separate campaign by the adversary, thereby multiplying cost, time and effort. The government could also consider a series of other measures including better surveillance and reconnaissance to prevent an attack on a satellite in the first instance. Lastly, India has a stated policy against weaponisation of outer space but the security compulsions are important factors for India to change the tack.[27] This means India needs to consider developing and demonstrating a debris-free ASAT option. In 2010, the Indian defence establishment issued a 15-year "Technology Perspective and Roadmap," that stated that India will demonstrate an ASAT capability by 2015; there has been no progress on that front, however.

India must also debate and explore various counter-space capabilities that it should develop as a means of deterrence. India should look at satellite jamming as an option in its basket of counter-space capabilities. It could explore a number of different jamming options available including proactive, function-specific or hybrid-smart jammers so as to produce the most effective results.[28] Some of the smart jammers would look at more selective spot or responsive jamming as well as deception in order to create effective responses. How jamming might be employed for different categories of satellites like at LEO, MEO, GEO and ground infrastructure must be explored, too. The use of lasers to blind reconnaissance satellites has been an effective jamming method, something that has been explored in India's own neighbourhood.[29]

Even as India explores all the different options in developing its counter-space capabilities, it must be emphasised that from a geostrategic perspective, jamming and such other technologies may not have the same impact as an ASAT test. Demonstrating an ASAT capability by destroying, say an old defunct satellite, may produce a far greater impact from a deterrence perspective. India could possibly undertake an ASAT in lower altitudes in order to avoid the debris issue.

CONCLUSION

India's reliance on outer space has grown immensely in the last few decades. As this dependence grows, so too do the vulnerabilities to adversarial attempts to sabotage and destroy India's capabilities, particularly from the relatively new threat of cyber warfare. Like most other countries, India's space capability is also tied to its social and economic growth story. Thus, any disruption or damage to its satellites can have a significant impact on the Indian economy and the society at large. Without a thorough assessment, there is no telling what a sophisticated hack could do to the country, or even the region. This rationale should give the government sufficient reason to institute multiple measures to test and safeguard its assets and infrastructure. The government has to bring about institutional and policy alterations to affect deterrence.

Developments such as China's ASAT test in 2007 and the US' shooting down of a satellite in 2008 have led to a more astute Indian policy approach. And there are important pending decisions such as the establishment of an aerospace command, for instance, which have been stuck with the Indian civilian bureaucracy. As anyone might imagine, technology is wildly outpacing this process and the cyber threats to India's space infrastructure are becoming increasingly sophisticated and potent as time goes by.

The political leadership has to take ownership of both the space and cyber domains and make the necessary institutional changes to secure India's interests. By all accounts, this might include the testing of offensive counter-space capabilities. However, India should weigh its options carefully. Testing a kinetic ASAT weapon such as a missile could create a significant cloud of space debris, such as China did and they have not stopped hearing about it since. Rather, it might be more politically expedient for India to develop softer weapons, such as its own cyber capabilities, in order to demonstrate its willingness to fight fire with fire.

Nevertheless, what is certain is that the kind of dillydallying that was witnessed with the Indian decision on nuclear testing should not be repeated in the outer space or cyber domains. Today, there are three countries – the US, Russia and China – that have demonstrated their anti-satellite capabilities. Interestingly enough, they are also the same three actors who are using cyber warfare capabilities most aggressively. India cannot wait for international legal processes to take effect in these domains.

ABOUT THE AUTHORS

Dr. Rajeswari Pillai Rajagopalan is Senior Fellow and Head, Nuclear and Space Policy Initiative, Observer Research Foundation.

Daniel A. Porras is an Associate for LMI Advisors (Washington, D.C.), completing his LLM in International Business and Economics Law at Georgetown Law.

ENDNOTES:

1. The United States did carry out an ASAT operation in 2008 but the satellite in question was destroyed as it was re-entering the Earth's atmosphere, no further space debris was created.
2. Yassir Hassan, 'Satellite Services and Interference-The current Situation', *ITU*, June 10, 2013, available at http://www.itu.int/en/ITU-R/space/workshops/2013-interference-geneva/presentations/Yasir%20Hassan-%20Arabsat.pdf.
3. 'Report to Congress of the U.S.-China Economic and Security Review Commission', *One Hundred and Eleventh Session*, November 2009, pg. 175.
4. Santamarta, Ruben, 'A Wake-up call for SATCOM Security', *IOACTIVE Technical White Paper* (2014); Libicki, Martin C., 'Brandishing Cyberattack Capabilities', *RAND National Defense Research Institute* (2013); Caroline Baylon, 'Challenges at the Intersection of Cyber Security and Space Security Country and International Institution Perspectives', *Chatham House*, The Royal Institute of International Affairs (2014); Matthew Kleiman and Sonia McNeil, 'Red Lines in Outer Space',*The Space Review*, March 5, 2012 available at http://www.thespacereview.com/article/2038/1.
5. 'The Space Industry Wakes up To Cyber Threat', *Interview* with Denis Bensoussan, Head of Space at Beazley, July 07, 2014, available athttp://www.lloyds.com/news-and-insight/news-and-features/market-news/industry-news-2014/the-space-industry-wakes-up-to-the-cyber-threat Bensoussan talks about jamming in addition to a range of threats and motivation behind these threats. Also see Maj Brian Garino, USAF, and Maj Jane Gibson, USAF, 'Space System Threats', Chapter 21, AU-18: *Space Primer* (US Air Command and Staff College, US Air University, 2009) available at http://www.au.af.mil/au/awc/space/au-18-2009/.
6. 'DPRK jamming GPS signals, says Seoul', May 3, 2012, available at http://www.northkoreatech.org/2012/05/03/dprk-jamming-gps-signals-says-seoul/; 'North Korea jamming' hits South Korea flights',*BBC News*, May 2, 2012, http://www.bbc.com/news/world-asia-17922021; Shaun Waterman, 'North Korean jamming of GPS shows system's weakness', *The Washington Times*, August 23, 2012, available at http://www.washingtontimes.com/news/2012/aug/23/ north-korean-jamming-gps-shows-systems-weakness/?page=all.
7. Disruptions in satellite services are nothing new. In one of the earlier instances, the LTTE managed to successfully hack a US Intelat satellite in order to broadcast pirated radio and television programmes to other countries. See 'Cyber-Hardening: Why It is Critical to Satellite Communications', *Thuraya*, available at http://www.thuraya.com/content/cyber-hardening-why-it-critical-satellite-communications.
8. 'BBC Fears Iranian Cyber-Attack over Its Persian TV Service', *The Guardian*, March 14, 2012, available at http://www.theguardian.com/media/2012/mar/14/bbc-fears-iran-cyber-attack-persian.
9. Peter Horrocks, 'Stop Blocking Now',*BBC News*, June 14, 2009, available athttp://www.bbc.co.uk/blogs/theeditors/2009/06/stop_the_blocking_now.html.
10. 'Egypt Jamming Al Jazeera's Satellite Signals', *Al Jazeera*, September 4, 2013, available at http://www.aljazeera.com/video/middleeast/2013/09/201393183256834226.html?utm=from_old_mobile.
11. Anthony Capaccio, 'Chinese Military Suspected in Hacker Attacks on US Satellites', *Bloomberg*, October 27, 2011, available at http://www.bloomberg.com/news/articles/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites; 'China denies it is behind hacking of U.S. satellites', *Reuters*, October 31, 2011, available at http://www.reuters.com/article/2011/10/31/us-china-us-hacking-idUSTRE79U1YI20111031.
12. See Les Johnson, 'Sky Alert: When Satellites Fail', *Springer*, 2013, p. 37, GoogleBooks, available at https://books.google.co.in/books?id=zVlDAAAAQBAJ&pg=PA37&lpg=PA37&dq=all+steps+required+to+command+the+satellite&source=bl&ots=qll4tDVATi&sig=Uq7kIUQQetbyoLT4n3V4q2isqZo&hl=en&sa=X&ved=0CCMQ6AEwAWoVChMI4eb9x__SxwIVkG2OCh0Rbgg1#v=onepage&q=all%20steps%20required%20to%20command%20the%20satellite&f=false.
13. Mary Pat Flaherty, Jason Samenow and Lisa Rein, 'Chinese Hack US Weather Systems, Satellite Network', *Washington Post*, November 12, 2014, available at http://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html.
14. 'Military and Security Developments Involving the People's Republic of China 2015', Annual Report to Congress by the *Office of the Secretary of Defence*, April 7, 2015.

15. Patrick S Poole, 'ECHELON: America's Secret Global Surveillance Network', 2000, available at http://web.archive.org/web/20070202171651/http://fly.hiwaay.net/~pspoole/echelon.html.
16. 'Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare', *Looking glass Cyber Threat Intelligence Group*, April 28, 2015.
17. 'The EpicTurla (snake/Uroburos) attacks', *KapinskyLabs*, availableat: http://www.kaspersky.com/internet-security-center/threats/epic-turla-snake-malware-attacks; Nakashima, Ellen, 'Russian hacker group exploits satellites to stea data, hidetracks', *The Washington Post*, September 9, 2015; Apps, Peter and JimFinkle, 'Suspected Russian spywareTurla targets Europe, UnitedStates', *Reuters*, March 7, 2014.
18. Pollock Richard, 'These are the hacker groupseveryoneiswatching right now', *The DailyCaller*, July 9, 2015,availableat http://dailycaller.com/2015/07/09/these-are-the-hacker-groups-everyones-watching-right-now/.
19. New IT Rules were brought in April 2011 under the IT Act 2000. See Gazette Notification, GSR 314(E): *Information Technology (Intermediaries guidelines) Rules*, 2011, April 11, 2011, available at http://deity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf.
20. 'National Cyber Security Policy-2013', Department of Electronics and Information Technology (DeitY), *Ministry of Communication and Information Technology, Government of India*, July 2, 2013, available at http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf.
21. KK Mookhey, 'India's National Cyber Security Policy – Implications for the Private Sector',*Network Intelligence* – ISO 27001 Certified, available at http://niiconsulting.com/checkmate/2013/07/indias-national-cyber-security-policy-implications-for-the-private-sector/#sthash.1NaIlxAU.dpuf.
22. Varun Aggarwal, 'GulshanRai becomes first chief of cyber security; post created to tackle growing e-threats',*The Economic Times*, March 4, 2015, available at http://economictimes.indiatimes.com/articleshow/46449780.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.
23. Analysts also predict even more serious and direct threats in the form of missiles launched into space targeting a satellite or a bomb placed on low Earth orbit with a timer or remote control.
24. Ruben Santamarta, 'A Wake-up Call for SATCOM Security', *Technical White Paper*, IOActive, 2014, available at http://www.ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf.
25. Andrea Gini, 'Cyber Crime – From Cyber Space to Outer Space', *Space Safety Magazine*, February 14, 2014, available at http://www.spacesafetymagazine.com/aerospace-engineering/cyber-security/cyber-crime-cyber-space-outer-space/.
26. 'Critical Infrastructure Protection: Commercial Satellite Security Should be More Fully Addressed', *US General Accounting Office*, Report to the Ranking Minority Member, Permanent Subcommittee on Investigations Committee on Governmental Affairs, US Senate, GAO-02-781-Commercial Satellite Security, August 2012, p. 22.
27. India's Defence Research and Development Organisation (DRDO) is reported to be developing mini-satellites for the purpose of battlefield deployment, should there be adversarial forces attack India's main satellites. See, 'Indian Defence's new target: Anti-Satellite Weapons', *IBC News Bureau*, September 6, 2015, available athttps://www.ibcworldnews.com/2015/09/06/indian-defences-new-target-anti-satellite-weapons/.
28. 'Jamming and Anti-jamming Techniques in Wireless Networks: A Survey', *International Journal of Ad Hoc and Ubiquitous Computing*, available at http://www.cs.montana.edu/yang/paper/jamming.pdf.
29. Benjamin Sutherland an analyst on the subject stated in an interview "There are lasers used to hit satellites, it's called dazzling, and it's a show of force. There are a handful of countries that can do it. China dazzles US and French satellites in low earth orbit not often, but regularly." He adds that these kinds of attack can actually damage some sensitive equipment. See Kevin Zambrano, 'Reporter for *The Economist* Holds Book Signing', *Independent*, January 21, 2012, available at http://www.independent.com/news/2012/jan/21/reporter-em-economistem-holds-book-signing/; Phillip C Saunders and Charles D Lutes, 'China's ASAT Test Motivations and Implications', National Defense University, *Institute for National Strategic Studies*, Washington DC, 2007, available at http://www.dtic.mil/dtic/tr/fulltext/u2/a517485.pdf; Phillip C. Saunders, 'China's Future in Space: Implications for US Security', *Space.com*, May 24, 2005, available at http://www.space.com/1116-chinas-future-space-implications-security.html.

OBSERVER RESEARCH FOUNDATION
Ideas • Forums • Leadership • Impact

ORF, 20, Rouse Avenue Institutional Area, New Delhi - 110 002, INDIA
Ph. : +91-11-43520020, 30220020. Fax : +91-11-43520003, 23210773
E-mail: contactus@orfonline.org
Website: www.orfonline.org